Computer Networks

Pithirat Horvichien, Natalie Lowe, Adit Mohan, Bruno Hasenfratz,

Dev Mistry, Guy Levy

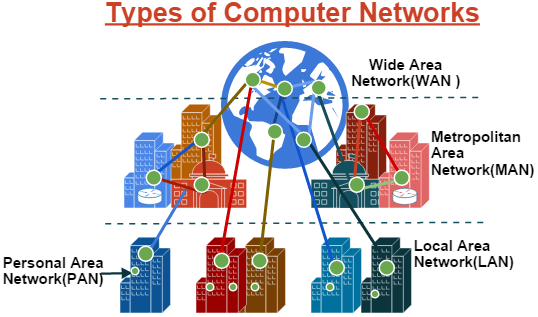
A **Computer Network** is a group of devices, which are connected by communication links that are built using physical media. Devices can be computers, telephones or anything able to send or receive message. [1]

The **Internet** is a network of computer networks, which allows transfer of information in an electronic format across the globe in a very short time period. On the other hand **Intranet** is the application of Internet technologies on a smaller scale e.g. university, college, hospital etc. [2]

**Client-Server Architecture** is a form of technology that separates computers and software into two groups: servers and clients. The client provides the interface and application processing, and the server provides the storage capacity, data processing and graphics. For example, every computer connected to a website acts as a client, while the websites computer acts as a server. [3]

A **Peer-to-Peer** system uses the **FTP** (File Transfer Protocol) whereby the client of one side contacts the server of the other side and a file is transmitted accordingly. This differs from client-server architecture as peers are equally privileged in their application.

**PAN** (Personal Area Network) is a network covering a very small area, such as a single room. The best-known example of this is Bluetooth and USB technology. PAN also includes WiFi as it can be used over a small area. **LAN** (Local Area Network), covers small areas such as offices and homes. This connection is mainly based on Ethernet, which can be supplied by twisted-pair cables or wireless routers. **WAN** (Wide Area Network) covers larger areas such as multiple buildings or a college campus. The largest use of WAN is the Internet; this can be used via fibre-optic cable or wirelessly via infrared transmission or microwave technology. **MAN** (Metropolitan Area Network) connects devices in the same metro area. For example, a company located in Brno may have offices in Prague and Plzen; all of their devices may be connected using MAN. This is mainly done using microwave transmission technology. [4]



**IP** stands for Internet Protocol address and is a numeric name assigned to each device participating in the computer/internet network.

Two versions of the Internet protocol are in use: **IP-version 4 (IPv4)** and **IP-version 6 (IPv6)** and each version is different from the other in the way they define the address.

The original system called **IPv4** (still used nowadays) constitutes 32-bits number, and was lunched in 1983.

The newer version of the IP is version 6, which constitution out of 128 bit number.

The **IPv6** was developed by the Internet Engineering Task Force (Organization for internet repair and maintain the internet; it’s a volunteer organization) to deal with the long- anticipated problem of IPv4 address exhaustion. [5]

IPv6 compared to IPv4:

• Larger address space

• Multicasting

• Stateless address autoconfiguration (SLAAC)

• Network-layer security

• Simplified processing by routers

• Mobility

• Options extensibility

• Jungbograms

• Privacy

In general, a **domain name (address)** represents an Internet Protocol resource, such as a personal computer used to access the Internet, a server computer hosting a web site, or the web site itself or any other service communicated via the Internet. In 2015, 294 million domain names had been registered. Domain names are used to establish a unique identity. Organizations can choose the domain name that corresponds to their name, hoping the Internet users to reach them more quickly and easily.

An often-used analogy to explain the **domain name system (DNS)** is that it serves as the „phone book“ of the Internet by translating computer hostnames into to IP addresses. For example, the domain name www.cookie.com translates to the address 93. 183. 255. 117 (IPv4) and 2700:2800:220:7b:25bf:1453:1994:aa7 (IPv6). In difference from a phone book DNS can be rapidly updated, allowing the IPs location on the network to change without effecting any online users, whom continually using hostnames.

A **Media Access Control address (MAC address)** of each computer is a unique identifier assigned to network interface for communications, usually used in WIFI, local area network (LAN). MAC addresses are often assigned by manufacturer of the computer and is a specific identity of the computer. The MAC address can been seen by the internet host (ISP: Internet service provider). [6]

Common **Internet Attack** methods include **Eavesdropping** (secretely listening to a private conversation without consent, usually between hosts on a network (e.g. the FBI have been accused of using programs to eavesdrop on suspicious people)). **Phishing** (an attempt to obtain sensitive information (e.g usernames and passwords, credit card details) by masquerading as a trustworthy entity in an electronic communication). **DoS** (Denial of service attack; overloading a network by flooding it with useless traffic. Two types, this normal type and DDoS (Distributed DoS) where several computers flood a system with packets in a co-ordinated fashion). **Viruses** (a piece of code which can copy itself and typically has a detrimental effect such as destroying data. Must attach itself to an existing program). **Worms** (Standalone malware program that replicates itself and spreads to other computers, often using a network to spread itself). **Trojans** (A program, usually a virus hidden inside a harmless-looking file or program. It isn’t activated until the file is opened, where it then causes damage). **Email Bombing** (sending huge volumes of emails to an address in an attempt to overflow the mailbox or overwhelm the server). **Spamming** (use of electronic messaging systems to send messages or advertising repeatedly on the same site or to an email). **Cookies** (small files stored on a user’s computer. Designed to hold a small amount of data specific to a particular client or website). **Systems boot record infectors** (virus that inserts its starting code into the boot sector of a computer. When the computer tries to boot up, the virus goes into the computer memory and can gain control over basic operations).

|  |  |  |
| --- | --- | --- |
| Computer Security Attributes | Attack Methods | Technology for Internet Security |
| Confidentiality | Eavesdropping, Hacking, Phishing, DoS and IP Spoofing | IDS, Firewall, Cryptographic Systems, IPSec and SSL |
| Integrity | Viruses, Worms, Trojans, Eavesdropping DoS and IP Spoofing | IDS, Firewall, Anti-Malware Software, IPSec and SSL |
| Privacy | Email Bombing, Spamming, Hacking, DoS and Cookies | IDS, Firewall, Anti-Malware Software, IPSec and SSL |
| Availability | DoS, Email Bombing, Spamming and Systems Boot Record Infectors | IDS, Anti-Malware Software and Firewall |
|  |  |  |

There are many gateways to protect computers against network breaches; these include IDS, Firewall, Cryptographic Systems and Anti-Malware. **IDS** (Intrusion Detection Systems) is an extra protection measure designed to ward off computer intrusions. **Firewall** is the front line of defence. **Cryptographic Systems involves** the use of codes and ciphers to transform data into nonsense data while transferring it in order to keep it secure, this type of protection continues to advance as hackers catch up with it. **Anti-Malware** is used to detect Malware such as Trojans, worms and viruses and cure them if they’re present. The difference between firewalls and Anti-malware scanners is that firewalls control the information sent to and from the device and blocks sites that may install malware from accessing the device. Whereas Anti-Malware programs look for and remove any malware present on the device already. [7]

References;

**[1]** Ivan Marsic. (2010) Computer Networks: Performance & Quality of Service.

**[2]** Vithal, GV, and Waghmode, SS., Intranet and Internet

**[3]** <http://www.businessdictionary.com/definition/client-server-architecture.html>

**[4]** David Delony. (2013) LAN WAN PAN MAN: Learn the Differences Between These Network Types. Techopedia.com.

**[5] http://www.whatismyipaddress.com/mac-address**

**[6] macvendors.com/what-is-mac\_address**

**[7]** Daya, B., Network Security: History, Importance, and Future. University of Florida Department of Electrical and Computer Engineering.